Über die Gruppen $PSL_n(q)$, die eine Untergruppe von Primzahlindex enthalten

Von NOBORU ITÔ in Nagoya (Japan)

Herrn Professor Dr. Ladislaus Rédei zum 60. Geburtstag

Über Permutationsgruppen vom Primzahlgrad hat man schon lange gearbeitet. Doch scheint es uns, daß man bis jetzt noch zu wenig Beispiele davon kennt. Daher dürfte es nicht ohne Interesse sein, aus einigen bekannten Klassen von Gruppen diejenigen Gruppen auszuwählen und zu untersuchen, die sich als Permutationsgruppen von Primzahlgrad darstellen lassen.

In dieser Arbeit handelt es sich nur um zwei Probleme: (1) Wann enthält $PSL_n(q)$ eine Untergruppe von Primzahlindex? Dies wird in Satz 1 beantwortet. (2) Eine Gruppe $G = PSL_n(q)$ enthalte eine Untergruppe vom Primzahlindex l. Wie viele Klassen konjugierter Untergruppen vom Index l gibt es in G? Diese Frage wird in Satz 2 beantwortet.

Bezeichnungen. F_q: Galois-Feld mit q Elementen. $GL_n(q)$: die n-dimensionale volle lineare Gruppe über F_q. $SL_n(q)$: die n-dimensionale spezielle lineare Gruppe über F_q. $PSL_n(q) = SL_n(q)/\text{Zentrum}$: die n-dimensionale projektive spezielle lineare Gruppe über F_q.

§ 1.

Vorerst schicken wir einen Hilfssatz voraus:

Hilfssatz 1. *Sei G eine zweifach transitive Permutationsgruppe von Grade n und H eine Untergruppe von G, deren Index kleiner als n ist. Dann ist H transitiv.*

Beweis. Wir ordnen jeder Permutation von G ihre Permutationsmatrix zu und erhalten so die Permutationsdarstellung G^* von G. Sei χ^* der Charakter von G^*. Da G zweifach transitiv ist, zerfällt χ^* in den Hauptcharakter $1(G)$ von G und einen irreduziblen Charakter χ des Grades $n-1$ von G. ([4], (29. 9)). Sei s die Anzahl der Transitivitätsgebiete von H. Ist

$s=1$, dann sind wir fertig. Also sei $s>1$. Dann enthält χ^*, auf H eingeschränkt, den Hauptcharakter $1(H)$ von H mit der Vielfachheit s. Da $s>1$ ist, enthält χ auf H den Hauptcharakter $1(H)$ von H mit positiver Vielfachheit. Dann kommen nach dem Reziprozitätssatz von Frobenius χ und $1(G)$ in $1^*(H)$ wirklich vor. Da der Grad von $1^*(H)$ gleich $G:H$ ist, haben wir die Ungleichung $G:H \geqq 1+n-1=n$, was unsere Annahme $G:H<n$ widerspricht.

Satz 1. *Sei $q=p^s$ eine Primzahlpotenz, $n\geqq 2$ und $q>3$ für $n=2$. $PSL_n(q)$ enthalte eine Untergruppe vom Primzahlindex l. Dann gilt die Gleichung $l=\frac{q^n-1}{q-1}$. Insbesondere ist $n=r$ eine Primzahl, s wird eine Potenz von r und es gilt $q\not\equiv 1 \pmod r$. Es gibt drei Ausnahmen, die für $n=2$ und für $q=5, 7$ und 11 auftreten.*

Beweis. Wir betrachten $G=SL_n(q)$. Bekanntlich ist die Ordnung von G gleich $q^{\frac{n(n-1)}{2}}(q^n-1)\cdots(q^2-1)$ ([1], §99). Nach Voraussetzung enthält G eine Untergruppe H vom Index l. Sei $Z=Z_n(q)$ das Zentrum von G. Dann besteht Z aus allen Matrizen der Gestalt $\begin{pmatrix}\mu & & & \\ & \mu & & \\ & & \ddots & \\ & & & \mu\end{pmatrix}$ mit $\mu^n=1$, $\mu\in F_q$. Also hat Z die Ordnung $d=(n, q-1)$. Da G/Z bekanntlich einfach ist ([1], § 104), ist die Permutationsgruppe (G, H) über den rechtsseitigen Nebenklassen von G nach H zu G/Z isomorph. Also haben wir die folgende Aussage:

(*) Die Primzahl l teilt die Ordnung von G/Z zur ersten Potenz und jede Restklasse LZ $(L\in SL_n(q))$ der Ordnung l ist nur mit ihrer Potenzen vertauschbar.

Fall I: $l\neq p$. Sei $m>0$ die kleinste Zahl, die der Kongruenz $q^m\equiv 1 \pmod l$ genügt. Angenommen, es sei $m<n-1$. Dann gilt $m>1$. Denn wegen $n-1>m$ ist die Ordnung von G durch $(q^3-1)(q^2-1)$ teilbar. Also wenn $m=1$ ist, muß l in d aufgehen. Sonst teilt l die Ordnung von G/Z in höherer als der ersten Potenz. Sei also $d\equiv 0 \pmod l$. Wegen der Einfachheit von G/Z ist l nicht kleiner als 5. Da $n\equiv 0 \pmod d$ ist, folgt $n\equiv 0 \pmod l$, insbesondere $n\geqq 5$. Dann teilt l die Ordnung von G/Z wieder in höhere als der ersten Potenz. Das widerspricht (*). Daher ist $m>1$. Dann gibt es in G eine Matrix L der Ordnung l der Gestalt $L=\begin{pmatrix}E & 0\\ 0 & L_m\end{pmatrix}$ mit $L_m\in SL_m(q)$. L ist mit jeder Matrix aus G der Gestalt $A=\begin{pmatrix}A_{n-m} & 0\\ 0 & E\end{pmatrix}$ mit $A_{n-m}\in SL_{n-m}(q)$ vertauschbar. Das widerspricht (*).

Nun sei $m=n-1$ und $m>1$. Man setze $F_{q^m}=\langle\lambda\rangle$ und $f(x)=$ $=(x-\lambda)(x-\lambda^q)\cdots(x-\lambda^{q^{m-1}})=x^m-a_1x^{m-1}-\cdots-a_m$ mit $a_i\in F_q$. Es sind $\begin{pmatrix}\lambda & & & \\ & \lambda^q & & \\ & & \ddots & \\ & & & \lambda^{q^{m-1}}\end{pmatrix}$ und $A=\begin{pmatrix}a_1 & \cdots & a_{m-1} & a_m \\ 1 & & & \\ & \ddots & & \\ & & 1 & \end{pmatrix}$ in $GL_n(q^m)$ konjugiert. Dann gehört $L=\begin{pmatrix}A^{q-1} & 0 \\ 0 & 1\end{pmatrix}$ zu G und hat die Ordnung $\frac{q^m-1}{q-1}$. Nach (*) folgt daraus die Gleichung $\frac{q^m-1}{q-1}=l$. Sei G_1 die Untergruppe aller Matrizen der Gestalt $\begin{pmatrix}a_{11} & 0 & \cdots & 0 \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn}\end{pmatrix}$ aus G. Dann ist der Index von G_1 in G gleich $\frac{q^n-1}{q-1}=ql+1$. Wegen $(ql+1,l)=1$ gilt $G=G_1H$. Setze $H_1=H\cap G_1$. Dann gilt $G_1:H_1=l$. G_1 enthält einen elementar abelschen Normalteiler N der Ordnung $q^m=(q-1)l+1$, der aus allen Matrizen der Gestalt $\begin{pmatrix}1 & 0 & \cdots & 0 \\ a_{21} & & & \\ \vdots & & E & \\ a_{n1} & & & \end{pmatrix}$ von G besteht. Sei L eine l-Sylowgruppe von G_1. Daraus folgt $N^L=N\subseteqq H_1\subseteqq H$. Nun haben wir $G=LH$. Also enthält der Durchschnitt aller Konjugierten von H in G die Untergruppe $N>1$. Das widerspricht der Einfachheit von G.

Nun sei $m=1$ und $n=2$. Man setze $F_q=\langle\lambda\rangle$ und $L=\begin{pmatrix}\lambda & 0 \\ 0 & \lambda^{-1}\end{pmatrix}$. Dann hat LZ die Ordnung $q-1$ für $p=2$ und $\frac{q-1}{2}$ für $p>2$. Nach (*) gilt die Gleichung $l=q-1$ für $p=2$ und $l=\frac{q-1}{2}$ für $p>2$. Also besitzt H/Z die Ordnung $q(q+1)$. Da je zwei verschiedene p-Sylowgruppen von $GL_2(q)$ den Durchschnitt E haben, ist die Anzahl der p-Sylowgruppen von H/Z kongruent 1 (mod q) und daher enthält H/Z, nach dem Sylowschen Satz oder nach einem Satz von FROBENIUS ([4], (5.1)), einen Normalteiler N/Z der Ordnung q oder $q+1$. Wenn die Ordnung von N/Z gleich q ist, so ist N/Z nach dem Sylowschen Satz ein Normalteiler von G/Z, was der Einfachheit von G/Z widerspricht. Also ist die Ordnung von N/Z gleich $q+1$. Wenn H/Z keinen Normalteiler der Ordnung q besitzt, da je zwei verschiedene p-Sylowgruppen

von H/Z den Durchschnitt E haben, gibt es kein Element $(\neq 1)$ in einer p-Sylowgruppe von H/Z, das mit einem Element $(\neq 1)$ von N/Z vertauschbar ist. Also sind alle Elemente $(\neq 1)$ von N/Z in H/Z konjugiert und N/Z ist eine elementar abelsche Gruppe von Primzahlpotenzordnung und eine p-Sylowgruppe von H/Z ist zyklisch (vgl. [5], Satz 3). Daraus folgt $q=p$. Da l der größte Primzahlteiler der Ordnung von G/Z sein muß, ist das ein Widerspruch.

Schließlich sei $m=n$. Wir setzen wieder $F_{q^n}=\langle\lambda\rangle$ und $f(x)=$ $=(x-\lambda)(x-\lambda^q)\cdots(x-\lambda^{q^{n-1}})=x^n-a_1x^{n-1}-\cdots-a_n$ mit $a_i\in F_q$. Dann sind $\begin{pmatrix}\lambda & & & \\ & \lambda^q & & \\ & & \ddots & \\ & & & \lambda^{q^{n-1}}\end{pmatrix}$ und $A=\begin{pmatrix}a_1 & \cdots & a_{n-1} & a_n\\ 1 & & & \\ & \ddots & & \\ & & 1 & \end{pmatrix}$ in $GL_n(q^n)$ konjugiert. Da $\det A=\lambda^{\frac{q^n-1}{q-1}}$ ist, enthält G/Z ein Element der Ordnung $\frac{q^n-1}{d(q-1)}$. Nach (*) folgt daraus die Gleichung $l=\frac{q^n-1}{d(q-1)}$. Indem wir einen Satz von ZSIGMONDY [6] benützen, sehen wir leicht ein, daß $n=r$ eine Primzahl ist. Daraus folgt, daß $d=(r,q-1)$ gleich entweder 1 oder r ist. Zunächst sei $d=r$. Wieder sei G_1 die Untergruppe aller Matrizen der Gestalt $\begin{pmatrix}a_{11} & 0 & \cdots & 0\\ a_{21} & a_{22} & \cdots & a_{2n}\\ \vdots & \vdots & & \vdots\\ a_{n1} & a_{n2} & \cdots & a_{nn}\end{pmatrix}$ aus G. Dann ist der Index von G_1 in G gleich $\frac{q^r-1}{q-1}=lr$. Sei E_r ein r-dimensionaler Vektorraum über F_q. Dann kann man $G/Z=$ $=PSL_r(q)$ als eine Permutationsgruppe über der Menge aller eindimensionalen Unterräume von E_r betrachten. Dabei wird G_1/Z die Untergruppe derjenigen Elemente von G/Z, die die „Ziffer" $\langle(1,0,\ldots,0)\rangle$ festlassen. Diese Permutationsgruppe G/Z ist bekanntlich zweifach transitiv. Also ist nach Hilfssatz 1 H/Z transitiv. Daher haben wir $G=G_1H$. Daraus folgt $G_1:G_1\cap H=$ $=G:H=l$. Da die Ordnung von G_1 prim zu l ist, ist das ein Widerspruch. Also haben wir $d=1$.

Wäre $q\equiv 1 \pmod r$, dann würde $l=q^{r-1}+\cdots+1\equiv r\equiv 0 \pmod r$, $l=r$ und $q^{r-1}=1$ folgen. Also gilt die Inkongruenz $q\not\equiv 1 \pmod r$.

Es ist $\frac{p^{sr}-1}{p^s-1}=l$. Wäre s keine Potenz von r, so gäbe es einen echten Teiler t von sr, der kein Teiler von s ist. Nach einem Satz von ZSIGMONDY [6] gibt es eine Primzahl u, für die p zum Exponenten gehört. Dann würde u ein Teiler von l. Also muß s eine Potenz von r sein.

Fall II: $l=p$. Dann folgt unmittelbar $n=2$ und $q=p$ (vgl. (*)). Dann ist unsere Behauptung schon bekannt ([1], § 262). Doch möchten wir hier einen anderen Beweis angeben.

Sei $p\equiv 1 \pmod 4$. Nach einem Satz von BURNSIDE ([4], (11.7)) ist die Permutationsdarstellung (G, H) zweifach transitiv. Also enthält H eine Untergruppe K von Index $p-1$. Dann ist die Ordnung von K/Z gleich $(p+1)/2$ und daher ist K/Z eine Hall-Untergruppe von G/Z. Da G (wie oben) ein Element der Ordnung $p+1$ enthält, ist K/Z, nach einem Satz von WIELANDT [3], zyklisch. Wie oben ist K in $GL_2(p^2)$ mit $\left\langle \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^p \end{pmatrix}; \lambda^{p+1}=1 \right\rangle$ konjugiert. Sei $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} \lambda^i & 0 \\ 0 & \lambda^{pi} \end{pmatrix}=\begin{pmatrix} \lambda^j & 0 \\ 0 & \lambda^{pj} \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ mit $\lambda^i \neq \lambda^j$ und $ad-bc=1$. Dann folgt $a=d=0$ und $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^2=\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$. Andererseits ist jedes Element von G, dessen Ordnung gleich 4 oder ein Primteiler von $p(p-1)$ ist, zu einer Matrix der Gestalt $\begin{pmatrix} a & 0 \\ b & a^{-1} \end{pmatrix}$ konjugiert (in G). Sei $\begin{pmatrix} c & d \\ e & f \end{pmatrix}\begin{pmatrix} a & 0 \\ b & a^{-1} \end{pmatrix}=\begin{pmatrix} a & 0 \\ b & a^{-1} \end{pmatrix}\begin{pmatrix} c & d \\ e & f \end{pmatrix}$ mit $cf-de=1$ und $b\neq 0$ oder $a\neq a^{-1}$. Dann folgt $d=0$. Also ist die Ordnung von $\begin{pmatrix} c & d \\ e & f \end{pmatrix}$ ein Teiler von $p(p-1)$. Nun sei r ein Primteiler von $\frac{p+1}{2}$ und $K(r)$ die r-Sylowgruppe von K. Also ist jedes Element $(\neq 1)$ von $K(r)$ mit einem Element A von G, dessen Ordnung $p(p-1)$ teilt, nur dann vertauschbar, wenn $A=\pm\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ ist. Es sei $N(r)$ der Normalisator von $K(r)$ in G. Dann ist wegen der Einfachheit von G und nach dem Zerfällungssatz von BURNSIDE $N(r)\neq K$. Daher hat $N(r)$ die Ordnung $2(p+1)$. Wenn also $N(r)$ in H enthalten ist, haben wir, nach dem Sylowschen Satz, die Kongruenz $\frac{p-1}{2}\equiv 1 \pmod r$. Daraus folgt $p\equiv 3 \pmod r$. Da andererseits $p\equiv -1 \pmod r$ ist, folgt der Widerspruch $r=2$. Daher haben wir $N(r)\cap H=K$ und H/Z ist eine Frobeniusgruppe. Also umfaßt H/Z, nach einem Satz von FROBENIUS ([4], (5.1)), einen Normalteiler N/Z der Ordnung $p-1$ und alle von Eins verschiedenen Elemente von N/Z sind in H/Z konjugiert. Daraus folgt die Gleichung $p-2=\frac{p+1}{2}$ und $p=5$. Umgekehrt enthält $PSL_2(5)\cong A_5$ eine Untergruppe vom Index 5.

Sei $p\equiv 3 \pmod 4$. G_1 bezeichne die Untergruppe von G, die aus allen Matrizen der Gestalt $\begin{pmatrix} a & 0 \\ b & a^{-1} \end{pmatrix}$ besteht. Da der Index von G_1 in G gleich $p+1$

ist, haben wir $G = HG_1$ und $H:G_1 \cap H = G:G_1 = p+1$. Also enthält H eine Untergruppe K vom Index $p+1$. Dann ist die Ordnung von K/Z gleich $\frac{p-1}{2}$ und daher ist K/Z eine Halluntergruppe von G/Z. Da G ein Element der Ordnung $p-1$ enthält, ist K/Z nach einem Satz von WIELANDT [3] zyklisch. Andererseits enthält H wie im Falle $p \equiv 1 \pmod 4$ eine Untergruppe L vom Index $p-1$. Dann ist die Ordnung von L/Z gleich $\frac{p+1}{2}$.

G_2 sei die Untergruppe von G, die aus allen Matrizen der Gestalt $\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$ besteht. Sei m die Anzahl aller Involutionen in G/Z und m_1 und m_1' diejenigen in G_1/Z und in H/Z. Da (G, G_1) und (G, H) zweifach transitiv sind, gibt es Involutionen $\bar{I}(=IZ)$ und $\bar{I}'(=I'Z)$, die im Normalisator von G_2/Z bzw. von L/Z liegen, mit den Gleichungen $G/Z = G_1/Z + (G_1/Z)\,\bar{I}(G_1/Z)$ und $G/Z = H/Z + (H/Z)\,\bar{I}'(H/Z)$. Seien d und d' die Anzahlen der Elemente X in G_2/Z und in L/Z mit den Gleichungen $\bar{I}\bar{X}\bar{I} = \bar{H}^{-1}$ und $\bar{I}'\bar{X}\bar{I}' = \bar{X}^{-1}$. Dann bekommen wir die Gleichungen (vgl. [2]) $m = m_1 + pd = m_1' + (p-1)\,d'$. Da die Ordnung von G_1/Z ungerade ist, haben wir $m_1 = 0$. Der Normalisator von G_2/Z ist gleich $G_2\langle I\rangle/Z$; er ist also eine Diedergruppe. Daher enthält $G_2\langle I\rangle/Z$ genau $\frac{p-1}{2}$ Involutionen, und alle Involutionen in $G_2\langle I\rangle/Z$ sind konjugiert. Also haben wir $d = \frac{p-1}{2}$. Wir setzen $\alpha_1 = \langle(1\ 0)\rangle$ und $\alpha_2 = \langle(0,\ 1)\rangle$. Dann besitzt jede Involution in $G_2\langle I\rangle/Z$ die Zyklendarstellung $(\alpha_1\,\alpha_2)\cdots$. Da (G, G_1) zweifach transitiv ist, sind alle Involutionen in G/Z zu einander konjugiert. Nun haben wir die Gleichung $m_1' + (p-1)\,d' = \frac{p(p-1)}{2}$. Wir betrachten die Permutationsgruppe (G, H). Sei r die Anzahl der Ziffern, die bei einer Involution festbleiben. Da alle Involutionen konjugiert sind und da m' gleich der Anzahl aller Involutionen in G/Z ist, die „die Ziffer H/Z" festlassen, so haben wir die Gleichung $pm_1' = rm = \frac{rp(p-1)}{2}$. (Eine Ziffer wird bei m' Involutionen festgelaßen und es gibt p Ziffern. Eine Involution läßt r Ziffern fest und es gibt m Involutionen.)

G_2 liegt im Normalisator der p-Sylowgruppe $\left\langle \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\rangle$ von G. Nach einem Satz von WIELANDT [3] sind K/Z und G_2/Z konjugiert. Also liegt K im Normalisator einer p-Sylowgruppe von G. Daraus folgt, daß jede Permutation $(\neq 1)$ von K/Z genau eine Ziffer (H/Z) festläßt und K/Z genau zwei Transitivitätsgebiete der Länge $\frac{p-1}{2}$ besitzt. Sei $N(K)$ der Normalisator von K in G. Dann haben wir $N(K) \subseteqq H$. Der Normalisator von G_2/Z

ist gleich $G_2\langle I\rangle/Z$. Sei $\bar{I}''=I''Z$ eine Involution in $N(K)/Z$. Da K Zentralisator jedes Elementes $\left(\neq\pm\begin{pmatrix}1&0\\0&1\end{pmatrix}\right)$ von K ist und K/Z genau zwei Transitivitätsgebiete der Länge $\frac{p-1}{2}$ besitzt, läßt $\bar{I}''$ genau 3 Ziffern fest. Also haben wir $r=3$ und $m'=\frac{3(p-1)}{2}$. Folglich haben wir $d'=\frac{p-3}{2}$. Daher gibt es in L/Z genau zwei Elemente $\bar{X}$ mit der Eigenschaft $\bar{I}'\bar{X}\bar{I}'\neq\bar{X}^{-1}$. Also ist die Ordnung von $\bar{X}$ höchstens gleich 4.

Sei M eine 2-Sylowgruppe von L derart, daß $M\langle I'\rangle$ eine 2-Sylowgruppe von G ist. $M\langle I'\rangle$ ist eine verallgemeinerte Quaternionengruppe, da bekanntlich $\begin{pmatrix}-1&0\\0&-1\end{pmatrix}$ die einzige Involution in G ist. Also ist $M\langle I'\rangle/Z$ eine Diedergruppe. Wir setzen $\frac{p+1}{2}=2^{\alpha}u$ mit $(2,u)=1$. Dann wird $M\langle I'\rangle/Z$ durch zwei Elemente $\bar{A}$ und $\bar{B}$ mit $\bar{A}^{2^{\alpha}}=\bar{B}^2=1$ und $\bar{B}\bar{A}\bar{B}=\bar{A}^{-1}$ erzeugt. Man kann $\bar{I}'=\bar{B}\bar{A}^{\alpha}$ setzen.

Wenn $M/Z=\langle\bar{A}\rangle$ ist, gilt für jedes Element $\bar{X}$ aus M/Z die Gleichung $\bar{I}'\bar{X}\bar{I}'=\bar{X}^{-1}$. Also gibt es in L/Z ein Element $\bar{Y}$ der Ordnung 3, für das die Ungleichung $\bar{I}'\bar{Y}\bar{I}'\neq\bar{Y}^{-1}$ gilt. Wegen $\bar{I}'(\bar{I}'\bar{Y}\bar{I}')\bar{I}'=\bar{Y}$ folgt daraus $\bar{I}'\bar{Y}\bar{I}'=\bar{Y}$. Wegen $\bar{A}^{x}\bar{Y}\neq\bar{Y}^{\pm1}$ für $\bar{A}^{x}\neq1$ folgt weiter $\bar{I}'\bar{A}^{x}\bar{Y}\bar{I}'=\bar{Y}^{-1}\bar{A}^{-x}=\bar{A}^{-x}\bar{Y}$. Insbesondere gilt $\bar{Y}^{-1}\bar{A}^{-1}=\bar{A}^{-1}\bar{Y}$. Wenn $a\geqq2$ ist, folgt daraus $\bar{A}^2\bar{Y}=\bar{Y}\bar{A}^2$. Das widerspricht $\bar{Y}^{-1}\bar{A}^{-2}=\bar{A}^{-2}\bar{Y}$. Also haben wir $a=1$. Wenn $\{\bar{A}\}\{Y\}\neq L/Z$ ist, sei $\bar{Y}'$ ein Element aus $L/Z-\{\bar{A}\}\{\bar{Y}\}$, das eine zu 2 teilerfremde Ordnung hat. Wegen $\bar{Y}'\bar{Y}\neq\bar{Y}^{\pm1}$ ist, gilt $\bar{I}'\bar{Y}'\bar{Y}\bar{I}'=\bar{Y}^{-1}\bar{Y}'^{-1}=\bar{Y}'^{-1}\bar{Y}$. Dann muß die Ordnung von $\bar{Y}'$ gerade sein. Das ist ein Widerspruch. Also ist $L/Z=\{\bar{A}\}\{\bar{Y}\}$ und $\frac{p+1}{2}=6$, das heißt $p=11$.

Wenn $M/Z\neq\langle\bar{A}\rangle$ ist, gibt es in M/Z $2^{\alpha-1}$ Elemente der Gestalt $\bar{B}\bar{A}^{x}$. Für diese Elemente gilt $\bar{B}\bar{A}^{\alpha}\bar{B}\bar{A}^{x}\bar{B}\bar{A}^{\alpha}=\bar{B}\bar{A}^{2\alpha-x}\neq\bar{B}\bar{A}^{x}=(\bar{B}\bar{A}^{x})^{-1}$. Also haben wir $2^{\alpha-1}\leqq2$, daß heißt $a\leqq2$. Wenn $a=1$ ist, kann man annehmen, daß $M/Z=\langle\bar{A}\rangle$ ist. Also haben wir $a=2$ und $M/Z=\langle\bar{A}^2,\bar{B}\bar{A}^{\beta}\rangle$. Dann gilt $\bar{I}'\bar{B}\bar{A}^{\beta}\bar{I}'=\bar{B}\bar{A}^{\beta+2}$. Nun sei $\bar{X}\neq1$ ein Element aus L/Z mit einer ungeraden Ordnung. Wegen $\bar{B}\bar{A}^{\beta}\bar{X}\neq\bar{B}\bar{A}^{\beta},\bar{B}\bar{A}^{\beta+2}$ haben wir $\bar{I}'\bar{B}\bar{A}^{\beta}\bar{X}\bar{I}'=\bar{X}^{-1}\bar{B}\bar{A}^{\beta}=\bar{B}\bar{A}^{\beta+2}\bar{X}^{-1}$. Wegen $\bar{A}^2\bar{X}\neq\bar{B}\bar{A}^{\beta},\bar{B}\bar{A}^{\beta+2}$ haben wir ferner $\bar{I}'\bar{A}^2\bar{X}\bar{I}'=\bar{X}^{-1}\bar{A}^2=\bar{A}^2\bar{X}^{-1}$. Daraus folgt $\bar{X}^{-2}\bar{B}\bar{A}^{\beta}\bar{X}^2=\bar{B}\bar{A}^{\beta}$. Da die Ordnung von $\bar{X}$ ungerade ist, folgt daraus $\bar{X}^{-1}\bar{B}\bar{A}^{\beta}\bar{X}=\bar{B}\bar{A}^{\beta}$. Das ist ein Widerspruch. Also gibt es kein Element $\bar{X}\neq1$ aus L/Z mit einer ungeraden Ordnung. Deshalb haben wir $L/Z=M/Z$ und $\frac{p+1}{2}=4$, das heißt $p=7$.

Umgekehrt betrachten wir $SL_2(3)$ (und $SL_2(5)$). Da die Ordnung von $SL_2(3)$ gleich $48 \not\equiv 0 \pmod 7$ ist, hat $SL_2(3)$ zwei irreduzible treue Darstellungen des Grades 2 über einem algebraisch abgeschlossenen Körper der Charakteristik 7. Die Charaktere dieser Darstellungen liegen in F_7. Also enthält $SL_2(7)$ zwei nicht konjugierte $SL_2(3)$. Ebenso enthält $SL_2(11)$ zwei nicht konjugierte $SL_2(5)$.

Damit ist der Beweis von Satz 1 beendet.

§ 2.

Wir schicken einige Hilfssätze voraus:

Hilfssatz 2. *Wenn $n>2$ ist, so ist die Bedingung*

$$\left((q^{n-1}-1)\cdots(q^2-1),\ \frac{q^n-1}{q-1}\right)=1$$

äquivalent mit den Aussagen: (1) *n ist eine Primzahl und* (2) $q \not\equiv 1 \pmod n$.

Beweis. Wenn n nicht prim ist, setzen wir $n=n_1n_2$ mit $n_i>1$ $(i=1,2)$. Dann haben wir $\frac{q^n-1}{q-1}=\frac{q^{n_1n_2}-1}{q-1}=\frac{q^{n_1n_2}-1}{q^{n_1}-1}\cdot\frac{q^{n_1}-1}{q-1}$. Also teilt jeder Primteiler von $\frac{q^{n_1}-1}{q-1}$ gleichzeitig $(q^{n-1}-1)\cdots(q-1)$ und $\frac{q^n-1}{q-1}$. Daher ist $n=r$ eine Primzahl. Wenn $q\equiv 1 \pmod r$ ist, haben wir $\frac{q^r-1}{q-1}=$ $=q^{r-1}+\cdots+1\equiv r\equiv 0 \pmod r$. Also teilt r gleichzeitig $(q^{r-1}-1)\cdots(q^2-1)$ und $\frac{q^r-1}{q-1}$.

Umgekehrt sei n eine Primzahl und $q \not\equiv 1 \pmod n$. Sei l ein gemeinsamer Primteiler von $\frac{q^n-1}{q-1}$ und $(q^{n-1}-1)\cdots(q^2-1)$. Dann folgt $q^n\equiv 1 \pmod l$ und $q^x\equiv 1 \pmod l$ mit $x<n$. Da n prim ist, haben wir $q\equiv 1 \pmod l$. Deshalb haben wir $\frac{q^n-1}{q-1}\equiv n\equiv 0 \pmod l$ und $n=l$. Das ist ein Widerspruch.

Aus diesem Hilfssatze folgt unmittelbar der folgende

Hilfssatz 3. *Es sei $G=SL_n(q)$. G_1 bezeichne die Untergruppe von G, die aus allen Matrizen der Gestalt* $\begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}$ *besteht. G_1 ist genau dann eine Hall-Gruppe von G, wenn* (1) *n eine Primzahl ist und* (2) $q \not\equiv 1 \pmod n$.

Wir bemerken noch, daß in diesem Falle $Z=1$ ist. In der Tat ist die Ordnung von Z gleich $(n, q-1)=1$. Also haben wir $SL_n(q) \cong PSL_n(q)$.

Wir brauchen noch einen Hilfssatz:

Hilfssatz 4. *Sei $G=SL_n(q)$ und K eine über F_q irreduzible Untergruppe von G, die eine p-Sylowgruppe P von G enthält, wobei $q=p^s$ ist. Dann ist K transitiv, wenn man G als Permutationsgruppe auf der Menge aller eindimensionalen Unterräume des n-dimensionalen Vektorraumes $E_n(q)$ über F_q betrachtet.*

Beweis. Man kann annehmen, daß P aus allen Matrizen der Gestalt $\begin{pmatrix} 1 & & & \\ x_{21} & 1 & & \\ \vdots & & \ddots & \\ x_{n1} & & & 1 \end{pmatrix}$ besteht. Zunächst bestimmen wir die Transitivitätsgebiete von P. Sei T_k die Menge aller eindimensionalen Teilräume von $E_n(q)$, die eine Erzeugende der Gestalt $(x_1, \ldots, x_k, 0, \ldots, 0)$ mit $x_k \neq 0$ besitzen. Dann sind $T_1, T_2, \ldots, T_n$ die Transitivitätsgebiete von P. In der Tat haben wir $(0, \ldots, \overset{k}{\overset{\vdots}{0}}, 1, 0, \ldots, 0) \begin{pmatrix} 1 & & & \\ x_{21} & 1 & & \\ \vdots & & \ddots & \\ x_{n1} & & & 1 \end{pmatrix} = (x_{k1}, \ldots, x_{k\,k-1}, 1, 0, \ldots, 0)$. Nun läßt K die Vereinigungsmenge von $T_{i_1}, \ldots, T_{i_l}$ $(1 \leqq i_1 < \cdots < i_l < n)$ nicht fest. Denn setzen wir für jedes A aus K $A=\begin{pmatrix} \overset{i_l}{\boxed{B}}\,{}^{i_l} & C \\ D & F \end{pmatrix}$, dann folgt aus $(x_1, \ldots, x_{i_l}, 0, \ldots, 0) \begin{pmatrix} B & C \\ D & F \end{pmatrix} = (y_1, \ldots, y_{i_l}, 0, \ldots, 0)$, wobei x_j alle Elemente von F_q durchläuft $(j=1, \ldots, i_l)$, daß $C=0$ ist. Aber da K irreduzibel ist, gibt es ein A in K mit $C \neq 0$:

Satz 2. *Es sei $G=SL_n(q)$, $n>2$ eine Primzahl $q \not\equiv 1 \pmod{n}$. Dann enthält G genau zwei Klassen konjugierter Hall-Gruppen vom Index $\frac{q^n-1}{q-1}$.*

Beweis (I). Es gibt mindestens zwei Klassen konjugierter Hall-Untergruppen vom Index $\frac{q^n-1}{q-1}$. Sei G_1 die Untergruppe von G, die aus allen Matrizen der Gestalt $A=\begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}$ besteht. Wir ordnen jeder

Matrix A von G_1 die Matrix $(A')^{-1}$ zu, wobei A' die transponierte Matrix von A bezeichnet. Wegen $((AB)')^{-1}=(B'A')^{-1}=(A')^{-1}(B')^{-1}$ ist diese Abbildung ein Isomorphismus von G_1. Wir bezeichnen mit G_1^* das Bild von G_1. Betrachten wir G als Permutationsgruppe auf der Menge aller eindimensionalen Unterräume von $E_n(q)$, so ist G transitiv und G_1 ist die maximale Untergruppe von G, die die „Ziffer" $\langle(1, 0, \ldots, 0)\rangle$ festläßt. Nun ist G_1^* nicht zu G_1 konjugiert. Dazu genügt es zu zeigen, daß G_1^* keine „Ziffer" festläßt. G_1^* besteht aus allen Matrizen der Gestalt $\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ 0 & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ 0 & a_{n2} & \cdots & a_{nn} \end{pmatrix}$.

Angenommen, $\langle(x_1, x_2, \ldots, x_n)\rangle \neq 0$ wird von G_1^* festgelassen.

Die Matrizen $\begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & a_{kk}=1 & 1=a_{k,k+1} & \\ & & & & \ddots \\ & & & & & 1 \end{pmatrix}$ $(k=1, 2, \ldots, n-1)$ gehören G_1^*.

Aus $(x_1, \ldots, x_k, x_{k+1}, \ldots, x_n)\begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & a_{kk}=1 & 1=a_{k,k+1} & \\ & & & & \ddots \\ & & & & & 1 \end{pmatrix}=$

$=(x_1, \ldots, x_k, x_k+x_{k+1}, x_{k+2}, \ldots, x_n)$ folgt $x_k=0$ $(k=1, \ldots, n-1)$.

Wegen $n>2$ enthält G_1^* die Matrix $\begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & & 0 & -1 \\ & & & 1 & 0 \end{pmatrix}$. Aus

$(0, \ldots, 0, x_n)\begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & & 0 & -1 \\ & & & 1 & 0 \end{pmatrix}=(0, \ldots, 0, x_n, 0)$ folgt $x_n=0$.

Das ist ein Widerspruch.

(II) Es gibt genau zwei Klassen konjugierter Hall-Untergruppen vom Index $\frac{q^n-1}{q-1}$. Sei H eine beliebige Untergruppe von G mit den Index

$\frac{q^n-1}{q-1}$. Dann enthält H eine p-Sylowgruppe von G. Wenn H irreduzibel in F_q ist, so ist H transitiv nach Hilfssatz 4. Dann ist die Ordnung von H durch $\frac{q^n-1}{q-1}$ teilbar. Das ist ein Widerspruch. Also ist H reduzibel in F_q. Daher kann man annehmen, daß jede Matrix A von H die folgende Gestalt hat: $A=\begin{pmatrix} A_1 & 0 \\ * & A_2 \end{pmatrix}$, wobei der Grad von A_i gleich n_i $(i=1,2)$ ist, unabhängig von A aus H. Wenn $1<n_1<n-1$ gilt, so sei m eine Primzahl, die die Bedingung $q^{n-1}\equiv 1 \pmod m$, $q^\nu \not\equiv 1 \pmod m$ für $1 \leqq \nu < n-1$ erfüllt. Eine solche Primzahl existiert nach einem Satz von Zsigmondy [6], außer im Falle $q=2$ und $n=7$. Dann muß jedes Element der Ordnung m von H die folgende Gestalt haben: $\begin{pmatrix} E & 0 \\ * & E \end{pmatrix}$. Das ist ein Widerspruch. Daher ist $n_1=1$ oder $n_1=n-1$ und es gilt

$$\begin{pmatrix} & & -1 \\ 1 & \ddots & \\ & 1 & \\ 1 & & \end{pmatrix} \begin{pmatrix} a_{11} & \cdots & a_{1\,n-1} & 0 \\ \vdots & & \vdots & \vdots \\ a_{n-1} & \cdots & a_{n-1\,n-1} & 0 \\ a_{n1} & \cdots & a_{n\,n-1} & a_{nn} \end{pmatrix} \begin{pmatrix} & & 1 \\ 1 & \ddots & \\ & 1 & \\ -1 & & \end{pmatrix} = \begin{pmatrix} a_{nn} & & \\ 0 & & \\ & & * \\ 0 & & \end{pmatrix}.$$

Also ist H außer im Falle $q=2$ und $n=7$ entweder zu G_1 oder zu G_1^* konjugiert. Nun sei $q=2$ und $n=7$. Die Ordnung der Untergruppe, die aus allen Matrizen der Gestalt $\begin{pmatrix} \text{Grad } 2 & 0 \\ * & \text{Grad } 5 \end{pmatrix}$ besteht, ist nicht durch 7 teilbar. Weiter ist die Ordnung der Untergruppe, die aus allen Matrizen der Gestalt $\begin{pmatrix} \text{Grad } 3 & 0 \\ * & \text{Grad } 4 \end{pmatrix}$ besteht, nicht durch 31 teilbar. Andererseits ist die Ordnung von H durch $7\cdot 31$ teilbar. Daher gilt wieder $n_1=1$ oder $n_1=6$ und wir können den obigen Schluß wiederholen.

Damit ist der Beweis von Satz 2 beendet.

Sei $n=2$. Da dann G_1 und G_1^* zueinander konjugiert sind, gibt es nach Teil (II) des vorangegangenen Beweis nur eine einzige Klasse von Hall-Untergruppen vom Index $q+1$.

Nun fragen wir „wie stark transitiv" die Permutationsgruppen (G, G_1) sind. Nach BURNSIDE sind sie zweifach transitiv. Für $n>2$ sind sie aber nicht zweifach primitiv, das heißt, G_1 ist nicht primitiv als Permutationsgruppe auf den von $\langle(1,0,\ldots,0)\rangle$ verschiedenen Ziffern. Zum Beispiel besteht die Untergruppe G_2, die die Ziffern $\langle(1,0,\ldots,0)\rangle$ und $\langle(0,1,\ldots,0)\rangle$ festläßt, aus allen Matrizen der Gestalt $\begin{pmatrix} a_{11} & 0 & 0 & \cdots & 0 \\ 0 & a_{22} & 0 & \cdots & 0 \\ & & * & & \end{pmatrix}$. Sie ist enthalten in der

Untergruppe von G_1, die aus allen Matrizen der Gestalt $\begin{pmatrix} a_{11} & 0 & 0 & \cdots & 0 \\ a_{21} & a_{22} & 0 & \cdots & 0 \\ & & * & & \end{pmatrix}$ besteht; G_2 ist also keine maximale Untergruppe von G_1. Für $n=2$ und $q=2^s$ ist (G, G_1) bekanntlich dreifach transitiv. In Zusammenhang mit dieser Betrachtung und Satz 2 teilen wir den folgenden Satz mit:

Satz 3. *Sei G eine dreifach transitive Permutationsgruppe des Grades n auf der Menge $\{1, \ldots, n\}$ und H eine intransitive Untergruppe vom Index n. Dann ist $H=G_i$ für ein passendes i. Dabei bezeichnet G_i die maximale Untergruppe von G, welche die Ziffer i festläßt.*

Beweis. Aus dem Beweis von Hilfssatz 1 in § 1 folgt, daß H genau zwei Transitivitätsgebiete T_1 und T_2 hat. Sei n_k die Länge von T_k und $n_1 \leqq n_2 = n - n_1$. Sei $i \in T_1$. Dann haben wir $G_i : G_i \cap H = HG_i : H = HG_i : G_i = n_1 \leqq n - n_1$. Sei $n_1 > 2$. Da G_i zweifach transitiv ist, ist $G_i \cap H$ transitiv auf $\{1, \ldots, n\} - \{i\}$ nach Hilfssatz 1. Das ist ein Widerspruch. Deshalb muß $n_1 = 1$, und also $H = G_i$ sein.

Insbesondere bekommt man

Satz 4. *Sei G eine dreifach transitive Permutationsgruppe vom Primzahlgrad p und H eine Untergruppe vom Index p. Dann läßt H eine Ziffer fest.*

Literatur

[1] L. E. Dickson, *Linear groups* (Leipzig, 1901).

[2] N. Itô, Normalteiler mehrfach transitiver Permutationsgruppen, *Math. Zeitschrift*, **70** (1958), 165—173.

[3] H. Wielandt, Zum Satz von Sylow, *Math. Zeitschrift*, **60** (1954), 407—408.

[4] H. Wielandt, *Vorlesungen über Permutationsgruppen.* Ausarbeitung von J. André, (Tübingen, 1955).

[5] H. Zassenhaus, Über endliche Fastkörper, *Abh. Math. Sem. Hamburg*, **11** (1936), 187—220.

[6] K. Zsigmondy, Zur Theorie der Potenzreste, *Monatsh. f. Math. u. Phys.*, **3** (1892), 265—284.

(Eingegangen am 1. Februar 1960)

MATHEMATISCHES INSTITUT DER UNIVERSITÄT NAGOYA,
NAGOYA-CHIKUSA, JAPAN